Department of Homeland Security Daily Open Source Infrastructure Report for 11 July 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports the Navy is investigating how personal information on more than 100,000 Navy and Marine Corp aviators and air crew wound up on a publicly available Website for more than six months. (See item 14)
- CNN reports authorities in Utah ordered a Southwest Airlines co−pilot out of the cockpit of his Arizona−bound jet shortly before takeoff and then jailed him on suspicion of being under the influence of alcohol. (See item 20)
- The U.S. Centers for Disease Control and Prevention has concerns that the nation will not receive all the seasonal influenza shots it needs this fall after the Food and Drug Administration's warning over contamination issues against Sanofi Pasteur, the country's largest flu vaccine maker. (See item 28)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 10, Associated Press* — **WPS Resources buying Peoples Energy.** WPS Resources Corp. said Monday, July 10, it has agreed to buy Peoples Energy Corp. for stock worth about $1.52 billion in a deal that will create an energy company with regulated utilities serving four

Midwest states and non−regulated businesses in the Northeast U.S. and Canada. The combined company would have assets of $9.2 billion. Its regulated electric and natural gas operations will serve about 1.6 million natural gas customers and 477,000 electric customers.
Source: http://www.nytimes.com/aponline/business/AP−WPS−Resources−Peoples−Energy.html?_r=1&oref=slogin

2. *July 08, ABC 11 (NC)* — **Wake County, North Carolina suffers after power outage.** Progress Energy says 60,000 people in Cary and western Raleigh, NC, lost power around 7:30 p.m. EDT, Friday, July 7. Power had been restored for most customers within two hours, but lingering problems were affecting about 3,000 customers in Morrisville until 11:30 p.m. Progress Energy says the problem has been fixed and all customers are back up.
Source: http://abclocal.go.com/wtvd/story?section=triangle&id=434798 4

3. *July 07, Associated Press* — **PUC says Xcel could have prevented February outage.** The Colorado Public Utilities Commission recently released a report stating that Xcel Energy probably could have prevented a major February 18 power outage in Colorado had it responded more quickly and effectively to developing problems that day. The outage came on a day as temperatures plunged to 13 degrees below zero and left 371,370 Colorado customers without electricity. Some 240,000 phone calls to Xcel that day got busy signals, and the few callers that got through were given inaccurate or incomplete information about the outage, the PUC said. The commission urged Xcel to improve customer communication, develop better mechanisms to purchase natural gas when demand is expected to be high, set up an emergency response team at the corporate level, and figure out who has executive−level accountability to make improvements. Earlier this month, the company said its plans include a new telephone system to better handle customer calls; revised forecasting to better predict natural gas demand; and a new policy that requires power plants to check key mechanical systems when extreme temperatures are forecast to prevent shutdowns.
Report: http://www.dora.state.co.us/PUC/docket_activity/HighprofileD ockets/06I−118EG.htm
Source: http://www.centredaily.com/mld/centredaily/business/14989922 .htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 10, Seattle Post−Intelligencer* — **Propane leak forces road closure, evacuation.** A section of Aurora Avenue North and North 125th Street in Seattle, WA, reopened by Monday morning, July 10, after a propane gas leak late Sunday night closed it. The leak occurred at a Lowe's Home Improvement Warehouse and about 20 residents west of the area were evacuated as a result.
Source: http://seattlepi.nwsource.com/local/277032_gasleak09.html

5. *July 10, CBS 5 (CA)* — **Chemical leak prompts road closure.** A Hazmat spill Monday morning, July 10, closed Mattox Road near Foothill Boulevard in Castro Valley, CA, in unincorporated Alameda County. The truck was thought to be leaking either chlorine or hydrochloric acid.
Source: http://cbs5.com/local/local_story_191105654.html

[Return to top]

Defense Industrial Base Sector

6. *July 10, Aviation Week* — **General: Keep developing satellite technology, but get it out faster.** The U.S. Air Force should continue to push the boundaries of technology in satellite development, but at the same time step up the pace of getting the technology out faster, according to Lt. Gen. Michael A. Hamel, commander of the Air Force's Space and Missile Systems Center at Los Angeles Air Force Base, CA. Some have argued that one reason for big cost overruns and schedule slips in Air Force satellite programs has been a culture of pushing technology too hard. In prepared remarks, Hamel appeared to side with this approach, saying that one of the aspects of a "back to basics" strategy now being used by the Air Force in satellite development and acquisition is a "block or incremental" philosophy. One thing that led to the current problems, he said, was that in the 1990s, requirements were ambitious, and it became clear only later that it would take too long and cost too much to meet them all.
   Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/SAT07106.xml

7. *July 09, Voice of America* — **Report: Gaps in U.S. missile defenses.** A newly−released independent report has criticized the United States missile defense network, saying it does not do enough to protect Americans from attack. The four−year study was released Friday, July 7, by former Ambassador Henry Cooper, who headed the U.S. missile defense program in the 1990s. Published by the Institute for Foreign Policy Analysis, the report highlights vulnerabilities in the nation's defenses and the increasing threat posed by other nations.
   Full−text report: http://www.ifpa.org/pdf/IWGreport.pdf
   Source: http://www.voanews.com/english/2006−07−09−voa5.cfm

8. *July 09, Military* — **Marines seek support for space plane.** Unlike the Air Force, Navy and Army, all three of which sponsor expensive satellite programs, the cash−strapped Marines are pushing just one space concept. It's called Small Unit Space Transport and Insertion (SUSTAIN) and it's a reusable spaceplane meant to get a squad of Marines to any hotspot on Earth in two hours −− then get them out. The idea is to reinforce embattled embassies, take out terrorist leaders or defuse hostage situations before it's too late. This year, Defense Advanced Research Projects Agency (DARPA) launched a space plane program called Hot Eagle. Capitalizing on Space Ship One and Hot Eagle, the Marines are hoping to get a space transport into service soon. But Col. Jack Wassink, a former Marine Corps jet jockey, says the Corps can't go it alone. He's been working hard since 2003 to convince the sister services and the scientific community to get behind SUSTAIN.
   Source: http://www.military.com/features/0,15240,104739,00.html

9. *July 07, Government Accountability Office* — **GAO−06−838R: Contract Management: DoD Vulnerabilities to Contracting Fraud, Waste, and Abuse (Correspondence).** In recent years, the Department of Defense (DoD) has increasingly relied on goods and services provided by the private sector under contract. Since fiscal year 2000, DoD’s contracting for goods and services has nearly doubled, and this trend is expected to continue. In fiscal year 2005 alone, DoD obligated nearly $270 billion on contracts for goods and services. Given the magnitude of

the dollar amounts involved, it is essential that DoD acquisitions be handled in an efficient, effective, and accountable manner. In other words, DoD needs to ensure that it buys the right things, the right way. Enacted January 6, 2006, the National Defense Authorization Act for Fiscal Year 2006 required the Government Accountability Office (GAO) to review DoD's efforts to identify and assess the vulnerability of its contracts to fraud, waste, and abuse. GAO reviewed the areas of vulnerability that DoD faces with regard to contracting fraud, waste, and abuse, and the recent initiatives that DoD has taken to address these vulnerabilities, including actions DoD has taken in response to a March 2005 Defense Science Board report on management oversight in acquisition organizations.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−838R

[Return to top]

Banking and Finance Sector

10. *July 10, Computerworld* — **Visa, MasterCard unveil new security rules.** Visa U.S.A. and MasterCard International will release new security rules in the next 30 to 60 days for all organizations that handle credit card data, a Visa official said last week. The rules will be the first major update to the one−year−old Payment Card Industry (PCI) data security standard, which analysts said is slowly but surely being adopted. One set of PCI extensions is aimed at protecting credit card data from emerging Web application security threats, said Eduardo Perez of Visa. Other new rules will require companies to ensure that any third parties that they deal with, such as hosting providers, have proper controls for securing credit card data. Most existing PCI requirements focus on security at the network level, but many of the latest threats are on the application side, said Philippe Courtot of Qualys. So it makes sense to update PCI to protect against Web application threats such as SQL injection attacks, cross−site scripting flaws, error−handling problems and validation errors, he said.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=112332&taxonomyI d=17

11. *July 10, VNUNet* — **Cyber−criminals switch to VoIP vishing.** Traditional Web−based phishing attacks are evolving into sophisticated phone scams in a VoIP telephony version of phishing dubbed 'vishing'. The new technique has been used by criminals to harvest details of the three−digit CVV security code, expiration date and other essential ID information in addition to the user's credit card and account numbers. According to Secure Computing, 'vishing' scams usually begin when the criminal configures a war dialer (sequentially dialed regional phone numbers) to call numbers in a given region. When the phone is answered, an automated recording is played to alert the consumer that their credit card has suffered fraudulent activity and the consumer should call a phone number immediately. The phone number is often an 800 number with a spoofed caller ID of the financial company it is pretending to represent.
Source: http://www.vnunet.com/vnunet/news/2160004/cyber−criminals−ta lk−voip

12. *July 10, Websense Security Labs* — **Phishing Alert: Google Mail.** Websense Security Labs has received reports that a variant of Google phishing attacks are increasing in sophistication. Users are shown a spoofed copy of the Gmail login page with a message claiming, "You WON $500.00!" The message states that this prize money will be delivered to an e−Gold, PayPal,

StormPay, or MoneyBookers account of their choice. If users select an account, they are informed that this prize money is only available to "premium members" of "Gmail Games." The page states that "Gmail Games" membership requires an $8.60 registration fee, and then asks users to pay the registration fee or forfeit the $500 prize money. Users are directed to an actual payment site to deliver the registration fee.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =545

13. *July 10, Web Host Industry Review* — **Hackers exploit banking sites.** Web hosting provider Goldleaf Technology announced on Monday, July 10, that a recent phishing scam attempted to steal personal financial data from its clients' bank sites. According to the company, its 600 client bank sites were affected by the security compromise for periods from nine to 91 minutes on May 25 between 1:35 p.m. and 2:50 p.m. CST.
Source: http://www.thewhir.com/marketwatch/071106_Hackers_Exploit_Ba nking_Sites.cfm

14. *July 07, Reuters* — **Navy probes data leak on 100,000 sailors, Marines.** The Navy said on Friday, July 7, that it was trying to determine how personal information on more than 100,000 Navy and Marine Corp aviators and air crew wound up on a publicly available Website for more than six months. In a fresh case of private information on military personnel being compromised, the full names and social security numbers of both active and reserve members appeared on the Naval Safety Center Website last December. Those affected are believed to include any Navy or Marine Corp aviator who has served during the past 20 years. The same information was also disseminated late last year to Navy and Marine Corps commands on 1,083 program disks mailed out as part of the service's Web Enabled Safety Program. The Naval Safety Center removed the information from the Website on Thursday. The Navy said there was no evidence that any of the disseminated data has been used illegally. The service is notifying those affected and setting up a 24−hour call center. Safety center spokesperson Evelyn Odango said the problem appeared to be an errant file.
Source: http://news.com.com/Navy+probes+data+leak+on+100%2C000+sailo rs%2C+Marines/2100−1009_3−6091936.html?tag=cd.top

15. *July 07, Sophos* — **PayPal phone phish scam uses voice recording to steal money.** Experts at SophosLabs have warned of a new phishing e−mail that attempts to trick PayPal users into calling a phone number and parting with their credit card information. The e−mail, which purports to come from PayPal, claims that the recipient's account has been the subject of fraudulent activity. However, unlike normal phishing e−mails, there is no Internet link or response address. Instead, the e−mail urges the recipient to call a phone number and verify their details. When dialed, users are greeted by an automated voice. Once the credit card details are entered, the scammer is free to steal the information for their own gain. If incorrect card details are entered, a request for re−entry is made, further enhancing the legitimacy of the fraudulent telephone number, which is still live.
Source: http://www.sophos.com/pressoffice/news/articles/2006/07/payp alvox.html

[Return to top]

Transportation and Border Security Sector

16. *July 10, Associated Press* — **Iberia pilots strike during busy tourist season.** Pilots at Spanish airline Iberia began a weeklong strike Monday, July 10, forcing the cancellation of more than 200 flights and obliging travelers to seek alternative arrangements during a vacation season in one of Europe's top tourist destinations. Pilots fear Iberia's investment in CATair, a new low−cost carrier, will lead to job cuts and are demanding guarantees that their jobs are safe. Iberia denies it plans job cuts. The pilots union said negotiations with the airline had broken down early Monday after Iberia rejected the union's latest proposals. It was unclear how many of Iberia's 1,900 pilots would take part in the strike, but the airline feared that 1,500 flights and around 200,000 passengers could be affected over the seven days of the planned strike. Iberia spokesperson Jaime Perez Guerra said 220 flights were canceled Monday and an average of 240 a day would be scrapped for the rest of the week. The stoppage will cost Spain's flagship carrier 35 million euros ($44.7 million) in lost revenue, he said.
Source: http://www.usatoday.com/travel/flights/2006−07−10−iberia−str ike_x.htm

17. *July 10, Los Angeles Times* — **California's highway system: crowded, crumbling.** California's highways were once the nation's gold standard. But as the interstate highway network celebrates its 50th anniversary and the summer driving season accelerates, the state is known for something else: some of the busiest, most dilapidated, and under−financed roads in the country. Over the last several years, money for highway projects has virtually disappeared, the victim of budget crises, stagnant federal funding, and a gas tax that has not been raised in a decade. The state's transportation system −− especially its crumbling highway network −− has a long list of unfunded needs with a price tag of at least $140 billion, said Sunne Wright McPeak, secretary of the state Business, Transportation, and Housing Agency. For now, the state expects to spend $21 billion on road maintenance and improvement over the next five years. Additional money could come from $37.3 billion in bond measures on the November ballot −− the only new money proposed in the state's $116−billion infrastructure plan. Of that bond money, about $11.5 billion would go to highway and road projects across the state to patch a system that the California Transportation Commission describes as "a shambles."
Source: http://www.latimes.com/news/local/la−me−roads10jul10,0,3364173.story?coll=la−home−headlines

18. *July 10, Patriot−News (PA)* — **Train crash shows risk posed by chemicals.** The derailment of a freight train on Wednesday, July 5, near Hershey Park, PA, could have been worse. The tank cars containing chlorine and potassium hydroxide could have leaked. Had they done so, hundreds of people could have been exposed to fumes that could have burned their eyes or damaged their lungs. Both substances aboard the Norfolk Southern Corp. train are commonly used in industry, and they are among a myriad of toxic substances pulled by locomotives that run through the region every day. Even more are hauled by truck along the region's highways on their way to manufacturing centers up and down the East Coast. There are about 800,000 hazardous−material shipments every day nationwide, according to the U.S. Department of Transportation's Office of Hazardous Materials Safety. About 94 percent of those are by truck. Usually they slip by unnoticed until something goes wrong. "Approximately 15 percent of all commercial vehicles on the highway are transporting hazardous materials," said James Weakland, hazardous−materials manager for the state police Bureau of Patrol. The two most common are gasoline and fuel oil. Others include low−level radioactive materials or waste and explosives.
Source: http://www.pennlive.com/news/patriotnews/index.ssf?/base/new

s/1152409226123850.xml&coll=1

19. *July 10, Government Accountability Office* — **GAO−06−933T: Maritime Security: Information−Sharing Efforts Are Improving (Testimony).** Sharing information with nonfederal officials is an important tool in federal efforts to secure the nation's ports against a potential terrorist attack. The Coast Guard has lead responsibility in coordinating maritime information sharing efforts. The Coast Guard has established area maritime security committees—forums that involve federal and nonfederal officials who identify and address risks in a port. The Coast Guard and other agencies have sought to further enhance information sharing and port security operations by establishing interagency operational centers—command centers that tie together the efforts of federal and nonfederal participants. This testimony from the Government Accountability Office is a summary and update to the April 2005 report, Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention, GAO−05−394. It discusses the impact the committees and interagency operational centers have had on improving information sharing and identifies any barriers that have hindered information sharing.
Highlights: http://www.gao.gov/highlights/d06933thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−933T

20. *July 09, CNN* — **Southwest co−pilot arrested on alcohol charges.** Authorities in Utah ordered a Southwest Airlines co−pilot out of the cockpit of his Arizona−bound jet shortly before takeoff Sunday morning, July 9, and jailed him on suspicion of being under the influence of alcohol, FBI and airline officials said. Carl Fulton, 41, of Fort Worth, TX, faces federal charges of operating a plane under the influence of alcohol, said Special Agent Pat Kiernan, an FBI spokesperson in Salt Lake City. Fulton was slated to fly as the first officer on a Southwest flight from Salt Lake City to Phoenix. Transportation Security Administration screeners had him followed to the flight's departure gate after noticing Fulton smelled of alcohol while going through security about a half−hour before takeoff, Kiernan said.
Source: http://www.cnn.com/2006/US/07/09/pilot.arrested/index.html

21. *July 09, Washington Post* — **Brake system is focus in Russia crash probe.** Investigators examining the charred remains of a Russian airliner that skidded off a rain−slick runway and crashed Sunday, July 9, in Siberia, killing at least 124 people, are focusing on the possibility that the plane's hydraulic brake system failed upon landing, according to news reports. Preliminary data indicate that "after landing, the aircraft's brake system failed, causing the failure of the system's other mechanisms," an investigator told the Russian news agency RIA Novosti. "As a result, the aircraft became uncontrollable after landing." The Airbus A−310 operated by S7 Airlines −− formerly Sibir Airlines, Russia's second−largest carrier −− was carrying 204 people, including eight crewmembers and 14 children younger than 12, when it crashed Sunday morning in the city of Irkutsk, according to the Russian Emergency Situations Ministry. The crash was the second involving an Airbus in Russia in the past two months. On May 3, a plane operated by the Armenian national carrier, Armavia, crashed as it approached the Russian Black Sea resort of Sochi. The cause of that crash, which killed all 113 passengers and crewmembers, is still under investigation.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/09/AR2006070900138.html

22. *July 09, Government Accountability Office* — **GAO−06−404: Homeland Security: Contract Management and Oversight for Visitor and Immigrant Status Program Need to Be Strengthened (Report).** The Department of Homeland Security (DHS) has established a multibillion−dollar program—U.S. Visitor and Immigrant Status Indicator Technology (US−VISIT)—to control and monitor the pre−entry, entry, visa status, and exit of foreign visitors. To deliver system and other program capabilities, the program relies extensively on contractors, some of whom are managed directly by US−VISIT and some by other agencies (including both DHS agencies, such as Customs and Border Protection, and non−DHS agencies, such as the General Services Administration). Because of US−VISIT's heavy reliance on contractors to deliver program capabilities, GAO was asked to determine whether DHS has established and implemented effective controls for managing and overseeing US−VISIT–related contracts. The Government Accountability Office (GAO) is making recommendations to the Secretary of Homeland Security to ensure that effective contract management and financial controls are established and implemented both for contracts managed by the US−VISIT program office and for those managed by other agencies. In written comments on a draft of this report, DHS concurred with the recommendations. In oral comments, officials from other agencies provided comments aimed at clarifying selected GAO statements.
Highlights: http://www.gao.gov/highlights/d06404high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−404

[Return to top]

Postal and Shipping Sector

23. *July 10, DM News* — **USPS generates net income of $6.2 million in May.** The U.S. Postal Service (USPS) generated net income of $6.2 million before escrow allocation during May, according to financial and operating statements. The Civil Service Retirement System Funding Act required the USPS to place $3 billion in an escrow account by September 30, to cover the difference between the retirement costs before and after the law's implementation. The USPS said it is allocating $250 million monthly for purposes of reconciling its financial position. USPS revenue in May is 11.5 percent higher than the same period last year, and $66.9 million over plan. Total mail volume in May was 1.3 billion pieces, or 8.0 percent higher than the same period last year. With the exception of Periodical Mail and International Mail, all of the major mail categories posted volumes above levels last year.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/37418.html

[Return to top]

Agriculture Sector

24. *July 10, Stop Soybean Rust News* — **Soybean rust found in Louisiana.** Friday, July 7, Louisiana officials found Asian soybean rust in Iberia Parish. There are now 24 counties in five U.S. states to have confirmed soybean rust this year. Iberia Parish touches the southeast corner of Lafayette Parish, where rust was found on kudzu June 30. The new find is about five miles from that first confirmed site, according to Clayton A. Hollier, Louisiana State University plant

pathologist. Neither parish had soybean rust last year −− the only rust in Louisiana in 2005 was in two parishes to the northeast, in East Baton Rouge Parish and Tangipahoa Parish.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=876

25. *July 10, Virginia Polytechnic Institute and State University* — **Vaccine developed for swine disease.** Researchers working in the Virginia−Maryland Regional College of Veterinary Medicine's Center for Molecular Medicine and Infectious Diseases at Virginia Tech have developed a vaccine to protect against Post−weaning Multi−systemic Wasting Syndrome (PMWS) in pigs, a major threat to the global swine industry. PMWS, caused by the Porcine Circovirus Type 2 (PCV2), has plagued the swine industry for almost ten years. By disrupting an animal's immune system, the virus renders the pig susceptible to a range of clinical disorders and severely constrains weight gain and development. First identified in the early 1990's, PMWS has been a major problem in Europe and Asia and recent outbreaks of PCV2−associated disease, with mortality rates as high as 30 percent, have been reported in the U.S. and Canada. The virus can cause significant disease in 30 to 50 percent of the animals it infects, causing major problems for production agriculture.
Source: http://www.newswise.com/articles/view/521788/

[Return to top]

Food Sector

26. *July 09, WKRC (OH)* — **Two dead, one hurt after plant explosion.** A second worker has died from his injuries after several explosions ignited a fire at a processing plant in Carthage, OH, Saturday, July 8. One worker remains hospitalized in critical condition. Fire investigators say one man died inside the building Saturday, which is owned by Origo −− a Minnesota company that processes fat for animal feed.
Source: http://www.wkrc.com/news/local/story.aspx?content_id=B7C70079−EF22−46A3−B5B1−27D640CCB61A

27. *July 07, Reuters* — **Codex sets new standards on lead, cadmium, aflatoxins.** Food experts on Friday, July 7, set new international standards on maximum allowed levels of contaminants including lead and cadmium, as well as aflatoxins, officials said. The standards, issued by the Codex Alimentarius Commission, are voluntary for countries, but apply to food consignments that move in international trade. Officials from 110 countries took part in the annual week−long talks. Codex is a joint food standards body run by two United Nations agencies −− the World Health Organization (WHO) and the Food and Agriculture Organization (FAO).
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−07−07T144116Z_01_L0782665_RTRIDST_0_HEALTH−FOOD−DC.XML&archived=False

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health Sector

28. *July 10, Atlanta Journal Constitution* — **Flu vaccine problems possible this fall.** The U.S. Centers for Disease Control and Prevention (CDC) has "heightened concern" that the nation will not receive all the seasonal influenza shots it needs this fall after the U.S. Food and Drug Administration's (FDA) stern warning over contamination issues against Sanofi Pasteur, the country's largest flu vaccine maker. Sanofi, which is producing 50 million doses of injectable influenza vaccine at its Swiftwater, PA, manufacturing plant, was warned by FDA for what the agency called "a number of significant objectionable conditions" at the plant. Among them were findings that 11 lots of Fluzone concentrate used to make the seasonal flu doses were contaminated with an unnamed microbe, out of 250 to 300 lots needed to make the promised vaccine. The FDA would not identify the contaminant but agreed with Sanofi that the problem appeared unlikely to prevent Sanofi Pasteur from making its 50 million doses. That amount is about 40 percent of the 120 million total flu shots expected for the U.S. this year.
Source: http://www.ajc.com/health/content/health/stories/0710fluvacc ine.html

29. *July 10, Guardian (United Kingdom)* — **Vaccine against lethal strain of avian flu ready for human testing.** A British drug company is seeking permission to conduct the first human trials of an experimental vaccine against the avian flu virus. The vaccine will target the lethal H5N1 strain of avian flu, which has spread rapidly throughout bird populations in Asia and has been brought to Europe by flocks of migrating waterfowl. Health officials fear the virus could mutate into a form easily transmissible between humans, potentially triggering a pandemic. Plans for the trial have been submitted to the Medicines and Healthcare Products Regulatory Agency, which is expected to give the green light for the trial to proceed at a London hospital. A vaccine against avian flu could significantly bolster efforts to limit the infection's spread if a pandemic strain emerges, by adding to government stockpiles of anti−viral drugs. Unlike conventional vaccines, which use weakened strains or fragments of the harmful virus, the test vaccine uses strands of DNA that can be made quickly and cheaply. In the trial, volunteers will be vaccinated using an alternative to a needle. Instead, a handheld device will blast harmless, microscopic gold particles coated in the vaccine into the upper arm at supersonic speeds.
Source: http://www.guardian.co.uk/uk_news/story/0,,1816694,00.html

30. *July 08, Voice of America* — **Communications tested in major bird flu exercise.** The 21 members of the Asia Pacific Economic Cooperation group have ended a major bird flu disaster exercise in Australia, testing how well various countries would communicate during a pandemic. It was the first time an exercise of this scale has been held involving the major economies of the Asia−Pacific region, including China, Japan and the United States. Participants were faced with a hypothetical outbreak of the deadly H5N1 virus among fishermen in an unidentified Asian village, which then leads to human−to−human transmission. It was a test of how countries could coordinate and cooperate in a serious outbreak. The simulation was held in Canberra and organized by Australia and Singapore. It began Wednesday, July 5, and ended Thursday, July 6. The results will be discussed at a summit in Singapore in August.
Source: http://www.voanews.com/english/archive/2006−06/2006−06−08−vo a8.cfm?CFID=28617163&CFTOKEN=15862288

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *July 09, Richmond Times−Dispatch (VA)* — **Storm evacuation to be difficult in Hampton Roads, Virginia.** Evacuating Hampton Roads, VA, in the face of a major hurricane will be a short−fused, fast−paced, come−as−you−are operation. As many as half of the region's 1.4 million people will have to leave in an estimated 300,000 vehicles, most of them exiting on an Interstate 64 that is regularly gridlocked with a fraction of that traffic. A slew of state agencies, local governments and private companies will have to work together smoothly to bring off an evacuation they will never be able to practice in real life before people need to go. And not everyone will be able to make it out before that storm hits, the state warns. "A traffic evacuation of the Hampton Roads area will be difficult," the state's hurricane emergency plan says. "More than 27 hours will be needed to completely evacuate potential traffic volumes generated by the at−risk population." But because many variables affect a storm's track, size, intensity and speed, the plan says, Virginia may not have enough time to evacuate everyone who decides to flee. Virginia emergency managers estimate that a major hurricane could force 600,000 to 700,000 people −− driving 300,000 cars and trucks −− to seek shelter inland.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&%09s=1045855934842&c=MGArticle&cid=1149189030247&path=%21news

32. *July 09, Associated Press* — **Hampton Roads law enforcement to get gamma ray detectors.** Law enforcement agencies in Hampton Roads, VA, are getting a new tool to alert first responders of a terrorist attack or industrial accident. The alarm systems will alert officials of gamma radiation, an invisible, odorless, and potentially deadly substance. "Unless you have this capability, you wouldn't know that you are responding to a scene that may have been a dirty bomb," said Bill Ginnow, a program manager with the Hampton Roads Metropolitan Medical Response System. The radiological equipment and 550 detectors were purchased with $400,000 of a federal homeland security grant. The devices will be distributed based on population to 10 cities and six counties in Hampton Roads within the next two months.
Source: http://hosted.ap.org/dynamic/stories/V/VA_GAMMA_RADIATION_ALARMS_VAOL−?SITE=VANOV&SECTION=STATE&TEMPLATE=DEFAULT&CTIME=2006−07−09−14−05−33

33. *July 09, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** State Disaster Emergency Declared, Sunday, July 9: Colorado Governor Bill Owens has issued an order for a state disaster emergency in counties hard−hit by recent rains and flooding. Douglas County is in the worst shape, with five homes flooded and 40 more threatened. Heavy rains Friday night destroyed at least three homes near

the town of Deckers, CO, southwest of Denver, and more precipitation is expected in that area. Earthquake Activity, Sunday, July 9: A strong 6.3 magnitude earthquake, part of a series of quakes between 5.0 and 6.1 in the last 24 hours, were reported in the vicinity of the Aleutian Islands, AK. No reports of damage or tsunami warnings issued.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat070906.shtm

34. *July 06, ABC News 4 (SC)* — **Bell South conducts disaster exercise.** Bell South conducted a large−scale disaster response exercise in Charleston, SC, to show off the company's processes and facilities. A mobile command center was set up that included a decontamination tent that would be used to work on telecommunication systems during an emergency. Part of the exercise involved the state's Ports Authority to ensure additional reliability of communications systems for Bell South and the Port.
Source: http://www.abcnews4.com/news/stories/0606/334033.html

35. *June 27, Department of Health and Human Services* — **HHS releases decision tool for emergency preparedness disclosures.** Emergency preparedness and recovery planners are interested in the availability of information they need to serve people in the event of an emergency. For example, planners seek to meet the special needs of the elderly or persons with disabilities in the event of an evacuation. The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule protects individually identifiable health information held by "covered entities." The information protected is referred to as protected health information (PHI). The HIPAA Privacy Rule permits covered entities to disclose PHI for a variety of purposes. The Department of Health and Human Services' (HHS) Office of Civil Rights has released a decision tool which presents avenues of information flow that could apply to emergency preparedness activities. The rules regarding the use and disclosure of PHI apply to all individuals; no special rules apply to particular populations, such as persons with disabilities.
Decision Tool: http://www.hhs.gov/ocr/hipaa/decisiontool/tool/
Source: http://www.hhs.gov/ocr/hipaa/decisiontool/

[Return to top]

Information Technology and Telecommunications Sector

36. *July 10, Thai News Agency* — **Warnings of 26 computer virus strains spreading over Asia.** Computer users in Thailand and other Asian countries have been warned of 26 computer virus strains spreading across the region via e−mails. The virus strains are worms in the RONTKBR.GEN family, which were first identified last year but have been spreading in wider areas across the region, according to manufacturer Trend Micro Incorporated. The worms are spreading through "no subject" e−mails, and had reportedly destroyed nearly 16,000 computers so far, the company warned in a statement released Sunday, July 9.
Source: http://etna.mcot.net/query.php?nid=23210

37. *July 10, VNUNet* — **Microsoft preps seven July security patches.** Microsoft plans to release seven security patches as part of its monthly security update Tuesday, July 11. Each patch

covers single or multiple vulnerabilities in one of the firm's software products.
Microsoft Security Bulletin Advance Notification:
http://www.microsoft.com/technet/security/bulletin/advance.m spx
Source: http://www.vnunet.com/vnunet/news/2159950/microsoft−preps−se ven−july

38. *July 07, Sophos* — **Gattman computer virus uses new method of infection.** Sophos researchers have discovered a proof−of−concept virus, called W32/Gattman−A, which works in a novel way. Unlike the majority of malicious software, which are Windows programs targeting the Windows operating system, this virus deliberately targets an analysis tool which is widely used by security researchers. The Gattman virus spreads through the program Interactive Disassembler Pro (IDA), produced by DataRescue. The Gattman virus, which is believed to have been written by members of the "Ready Rangers Liberation Front" and "The Knight Templars" virus−writing gangs, works by infecting IDC files. IDC is a script programming language similar to ANSI C, which allows researchers to customize and enhance the behavior of the IDA tool. They are often useful in unscrambling esoteric or hidden parts of malicious code, and are often exchanged with other researchers as part of the effort of taking apart a new piece of malware.
Source: http://www.sophos.com/pressoffice/news/articles/2006/07/gatt man.html

39. *July 06, Secunia* — **Microsoft Excel style buffer overflow vulnerability.** Nanika has reported a vulnerability in Microsoft Excel, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when handling overly long styles. This can be exploited to cause a buffer overflow by tricking a user into opening a specially crafted spreadsheet. Successful exploitation may allow execution of arbitrary code, but requires that the user chooses to repair the document (Excel 2002/2003) or clicks the "Style" option (Excel 2000). NOTE: The vulnerability only affects certain Asian language versions (e.g. Chinese) of the product.
Vulnerable: : Microsoft Excel 2000; Microsoft Excel 2002; Microsoft Excel 2003; Microsoft Office 2000; Microsoft Office 2003 Professional Edition; Microsoft Office 2003 Small Business Edition; Microsoft Office 2003 Standard Edition; Microsoft Office 2003 Student and Teacher Edition; Microsoft Office XP.
Solution: Do not open untrusted office documents.
Source: http://secunia.com/advisories/20268/

40. *July 06, Reuters* — **United Kingdom agrees to extradite alleged hacker to U.S.** Britain on Thursday, July 6, approved the extradition of a computer expert accused by the United States of perpetrating the world's "biggest military hack of all time." Gary McKinnon was arrested in June last year following charges by U.S. prosecutors that he illegally accessed 97 U.S. government computers, including the Pentagon, Army, Navy and NASA systems, and causing $700,000 worth of damage.
Source: http://news.com.com/U.K.+agrees+to+extradite+alleged+hacker+ to+U.S./2100−7348_3−6091493.html?tag=cd.top

41. *July 06, Associated Press* — **Gangs use Internet to showcase exploits.** Some of the country's most notorious street gangs have gotten Web−savvy, showcasing illegal exploits, making threats, and honoring killed and jailed members on digital turf. Crips, Bloods, MS−13, 18th Street and others have staked claims on various corners of cyberspace. George W. Knox,

director of the National Gang Crime Research Center, said he has trained hundreds of police officials in how to cull intelligence on gang membership, rivalries, territory and lingo from these Webpages. "In order to understand any subculture, be it al Qaeda, witches, devil worshippers or gangs, you have to be able to know their own language," Knox said. Knox said it's important for police to learn how to read between the lines on gang Websites and blogs. Time on the Web may help them understand arcane Web clues. Knox and others fear gangs are using the Internet to recruit new members.
Source: http://abcnews.go.com/US/wireStory?id=2161304

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of multiple vulnerabilities in Microsoft Internet Explorer (IE) 6.0. US−CERT is also aware of a public blog that will be posting new web browser bugs on a daily basis in July. US−CERT will be analyzing relevant vulnerabilities, as well as actively monitoring the site to provide additional information as it becomes available. Please review URL: http://metasploit.blogspot.com/2006/07/month−of−browser−bugs .html

Until an update, patch, or more information becomes available, US−CERT strongly recommends the following:

Disable ActiveX

Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Do not follow unsolicited links.

Review the steps described in Microsoft's document to improve the safety of your browser: http://www.microsoft.com/athome/security/online/browsing_saf ety.mspx

US−CERT will continue to update current activity as more information becomes available.

Public Exploit Code for Unpatched Vulnerabilities in Microsoft Internet Explorer

US−CERT is aware of publicly available exploit code for two unpatched

vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100: http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108): http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser: http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ: http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	37501 (−−−), 1026 (win−rpc), 445 (microsoft−ds), 38566 (−−−), 6588 (AnalogX), 6999 (iatp−normalpri), 24232 (−−−), 25 (smtp), 32790 (−−−), 4672 (eMule) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

42. *July 10, Associated Press* — **New York City building collapses after explosion, fire.** A four−story building housing doctors' offices collapsed and burned Monday, July 10, after what witnesses described as a thunderous explosion that rocked the neighborhood just off Madison Avenue. Authorities said the apparent cause was a gas explosion and that suicide was being investigated. At least 15 people were injured, including five civilians and 10 firefighters, the Fire Department said. A doctor who lived in the building, 66−year−old Nicholas Bartha, was pulled from the rubble after communicating with authorities from his phone in the wreckage, fire chief Nicholas Scoppetta said. Scoppetta said authorities were investigating the possibility that the blast was the result of a suicide attempt. A police official told the Associated Press that the lawyer for the doctor's wife contacted police recently and said that she had received an e−mail in which the physician indicated he was contemplating suicide. The building included two doctors' offices, and records show at least one apartment was in building, Fire Department Lt. Eugene Whyte said. Authorities said a nurse who was supposed to open one of the offices arrived late, narrowly missing the explosion. White House press secretary Tony Snow told reporters there did not appear to be a "terrorism nexus" related to the blast.
Source: http://www.usatoday.com/news/nation/2006−07−10−manhattan−bui lding_x.htm

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer